

TAMPER-PROOF COMPUTER SYSTEM

Publication number: JP2002251326

Publication date: 2002-09-06

Inventor: ITO SHINJI; YOSHIURA YUTAKA; OKAMOTO HIROO

Applicant: HITACHI LTD

Classification:

- international: G06F12/14; G06F21/00; G06F21/06; G06F21/22;
G06F21/24; G06K19/00; G06F12/14; G06F21/00;
G06F21/22; G06K19/00; (IPC1-7): G06F12/14;
G06F1/00; G06K19/00

- European: G06F21/00N7P5M2; G06F21/00N7D

Application number: JP20010045949 20010222

Priority number(s): JP20010045949 20010222

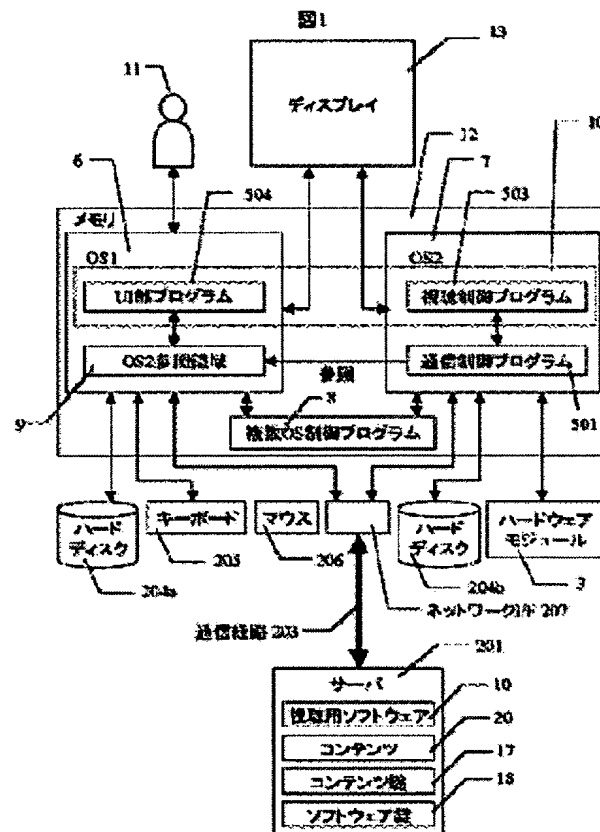
Also published as:

US2002116632 (A)

Report a data error he

Abstract of JP2002251326

PROBLEM TO BE SOLVED: To provide a system and a method on a PC for realizing a system capable of preventing static and dynamic analyses and alterations by a user of software that operates on a PC. **SOLUTION:** Two OSs being an OS1 that can be operated by a user and an OS2 that operates in the background are made to simultaneously operate on the PC. Audio-visual software 10 is prevented from being analyzed and tampered by the user 11 by operating the audio-visual software 10 on the OS2. Activation of the system and management of a key are also performed by using a hardware module 3. Furthermore, the OS1 indirectly accesses the OS2 by eliminating direct access from the OS1 to the OS2 and allowing the OS2 side to refer to the OS2 reference area 9 of the OS1 side.



Data supplied from the esp@cenet database - Worldwide

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2002-251326
(P2002-251326A)

(43) 公開日 平成14年9月6日 (2002.9.6)

(51) Int.Cl. ⁷	識別記号	F I	テーマコード* (参考)
G 0 6 F 12/14	3 2 0	G 0 6 F 12/14	3 2 0 E 5 B 0 1 7
			3 2 0 B 5 B 0 3 5
1/00		9/06	6 6 0 C 5 B 0 7 6
G 0 6 K 19/00		G 0 6 K 19/00	Q

審査請求 未請求 請求項の数 5 O L (全 15 頁)

(21) 出願番号 特願2001-45949(P2001-45949)

(22) 出願日 平成13年2月22日 (2001.2.22)

(71) 出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72) 発明者 伊藤 信治

神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所システム開発研究所内

(72) 発明者 吉浦 裕

神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所システム開発研究所内

(74) 代理人 100075096

弁理士 作田 謙夫

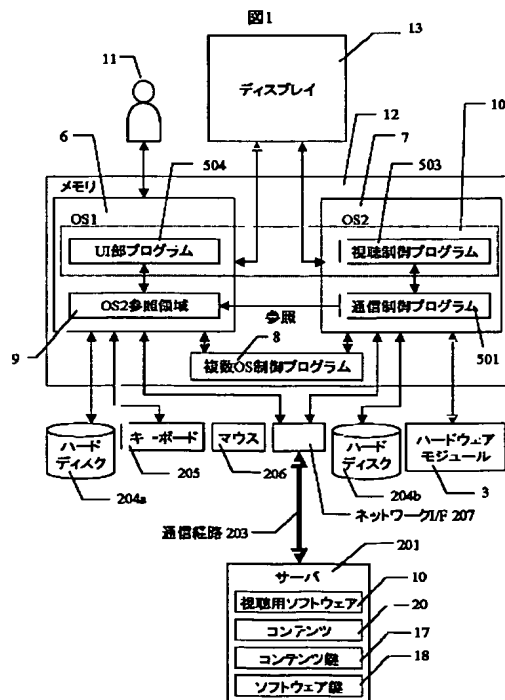
最終頁に続く

(54) 【発明の名称】 耐タンパ計算機システム

(57) 【要約】

【課題】 PC上で動作するソフトウェアのユーザによる静的及び動的な解析、改ざんを防止可能なシステムをPC上で実現するシステム及び方法を提供する。

【解決手段】 PC上にユーザが操作可能なOS1とバックグラウンドで動作するOS2の2つのOSを同時に動作させる。視聴用ソフトウェア10をOS2上で動作させることにより、ユーザ11による視聴用ソフトウェア10の解析、改ざんを防止する。また、ハードウェアモジュール3を用いて、システムの起動および鍵管理を行う。さらに、OS1からOS2への直接のアクセスをなくし、OS1側のOS2参照領域9をOS2側が参照することにより、間接的にOS1からOS2へアクセスを行う。



【特許請求の範囲】

【請求項1】CPUと主記憶装置とを有し、アプリケーションソフトウェアを動作させる耐タンパ計算機システムであって、

第1と第2のOSを備え、

上記アプリケーションソフトウェアは、上記第1のOS上で動作する第1の部分プログラムと、上記第2のOS上で動作する第2の部分プログラムとからなり、

上記第1の部分プログラムは、当該計算機のユーザから操作を受け付けて上記第2の部分プログラムへコマンドを発行するユーザインタフェース部を備え、

上記第2の部分プログラムは、上記第1の部分プログラムが発行したコマンドの内、予め許可されたコマンドを実行し、

上記ユーザによる上記第2の部分プログラムへのアクセスまたは解析を防止する耐タンパ計算機システム。

【請求項2】請求項1に記載の耐タンパ計算機システムであって、

上記第2の部分プログラムは、コマンドを実行するコマンド処理プログラムと、

上記コマンド処理プログラムに、第1の部分プログラムが発行したコマンドの内、特定の許可されたコマンドを上記コマンド処理プログラムに送信する通信制御プログラムと、を備える耐タンパ計算機システム。

【請求項3】請求項2に記載の耐タンパ計算機システムであって、

さらに、上記第1と第2のOSを制御する複数OS制御プログラムを備え、

上記複数OS制御プログラムは、上記通信制御プログラムが上記第1のOSが管理するメモリ領域の特定領域を参照可能になるように設定し、

上記第1の部分プログラムのユーザインタフェース部は、上記特定領域にコマンドを書き込むことによりコマンドを発行し、

上記通信制御プログラムは、上記特定領域を参照して、上記第1の部分プログラムが発行したコマンドを読みとり、上記第2のOSが管理するメモリ領域内に備える許可されたコマンドリストを参照して、上記許可されたコマンドを上記コマンド処理プログラムに送信する耐タンパ計算機システム。

【請求項4】請求項3に記載の耐タンパ計算機システムであって、

耐タンパ性を有し、システム起動プログラムを格納するハードウェアモジュールを接続し、

当該耐タンパ計算機システムは、起動時に上記ハードウェアモジュールから上記起動プログラムを読み出す初期プログラムを備え、

上記起動プログラムは、上記複数OS制御プログラムを読み出して実行させる機能と、

上記複数OS制御プログラムは、上記第1のOSと上記

第2のOSとを読み出して実行させる機能と、を備える耐タンパ計算機システム。

【請求項5】請求項4に記載の耐タンパ計算機システムであって、

上記第2の部分プログラムは、本体起動プログラムと暗号化ソフトウェアとデジタル署名とを備え、

上記ハードウェアモジュールは、上記暗号化ソフトウェアの復号化鍵と上記本体起動プログラムを認証する機能とを備え、

上記本体起動プログラムは、上記ハードウェアモジュールとの間で認証を行う機能と、上記ハードウェアモジュールから上記暗号化ソフトウェアの復号化鍵を取り出す機能と、取り出した上記復号化鍵を用いて上記暗号化ソフトウェアを復号化する機能と、を備え、

上記第1の部分プログラムから読み出したコマンドに従い、上記本体起動プログラムの実行と、上記暗号化ソフトウェアの復号化と実行とを行う耐タンパ計算機システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は計算機上で動作するソフトウェアの解析、改ざんを防止し、高い安全性を確保するための技術に関する。

【0002】

【従来の技術】動画、静止画、音楽などのデジタルコンテンツを視聴するための再生装置には、著作権保護機能を持った専用ハードウェアを用いる場合と、著作権保護機能を持った視聴用ソフトウェアを用いる場合とがある。視聴用ソフトウェアを用いる場合には、通常パーソナルコンピュータ（以下、PCという）のような汎用的計算機が再生装置として用いられるため、以下、PCを例にして説明する。

【0003】著作権保護機能を持った専用ハードウェアを用いた場合、コンテンツは暗号化して配布し、正規のプレーヤの、内部の解析、改ざんが困難な耐タンパモジュール内で暗号化コンテンツの復号を行い、利用条件などの付加情報の読み取りを行い、利用条件を満足する場合にのみ再生を行っている。

【0004】PC上で著作権を保護しつつコンテンツの視聴を行う場合、視聴用ソフトウェアに著作権保護機能を付加することによりコンテンツの再生を行う。具体的には、コンテンツのストリーミング配信の場合は、コンテンツをユーザのPC上に保存しないようにすることによって視聴する。または、暗号化されたコンテンツをユーザのPCに保存しておき、視聴するときは専用ハードウェアを用いる場合と同様に、暗号化コンテンツの復号、利用条件の読み取り、再生を行う。

【0005】

【発明が解決しようとする課題】視聴用ソフトウェアの著作権保護機能などの改ざん及び解析を防止するために

は、これを暗号化してファイルに保存する方法と隠しファイルのような見えないファイルに保存する方法がある。上記の二つの方法の実行時には、メモリ内で暗号が解かれ、実行時には、隠しファイルの内容がメモリにロードされる。そのため、実行時にメモリが解析されるといふ懸念がある。同様に、コンテンツの不正コピーを防止するためには、視聴用ソフトウェアの場合と同様に、これを暗号化してファイルに保存する方法と隠しファイルのような見えないファイルに保存する方法がある。これらの方法についても、視聴用ソフトウェアの場合と同様の懸念がある。

【0006】現状のPCは、専門の知識を持っている人であればオペレーティングシステム（OS）を操作したり、あるいは他のソフトウェアを導入することにより、ハードディスクなどに保存されている視聴用ソフトウェアを解析、改ざんを行うことが可能になる。そのため、保存できないように意図されているコンテンツを保存できるようにしたり、利用条件に反する利用を行ったり、あるいは私的利用のみ許されているコンテンツを他人が利用できるようにすることが可能であり、著作権を保護できなくなることが有り得る。

【0007】専用ハードウェアを用いた場合には十分に著作権を保護することは可能であるが、端末がモデルチェンジした場合や付加された新しい機能を使おうとした場合にはユーザは新しい端末を購入する必要があり、負担を強いられる。今後、ますます多機能化が進むと予想され、これらの問題を克服して専用ハードウェアを常に最新の機能を利用可能な状態にするのは困難である。

【0008】

【課題を解決するための手段】本発明は、PCのような汎用的な装置上で動作する視聴用ソフトウェアを用いてコンテンツを視聴するコンテンツ視聴システム（以下、単にシステムという）において、コンテンツの著作権をより厳重に保護可能な技術を提供する。本発明は、PCのような汎用的な装置上で動作する視聴用ソフトウェアの解析、改ざんを困難にする技術、システムを提供する。

【0009】本発明の一態様では、以下の構成を提供する。ユーザが操作を行うユーザインタフェース処理に係わる環境1と不正操作から保護したい環境2という独立した2つの環境とそれらを接続する通信機能をPCなどの一台の装置上に設ける。それぞれの環境上で動作する処理ユニット（プログラム）が連携してアプリケーションソフトウェア（たとえば視聴用ソフトウェア）を構成する。不正処理を排除するために、環境1から環境2または環境2から環境1への通信を制限する通信制御機能を設定する。具体的には、以下のように行う。

【0010】環境1から環境2への通信は、環境1側の視聴用ソフトウェアが通信のために設けた特定領域に、送信する命令または情報を書き込む。環境2側はこの特

定領域を参照することにより命令または情報を受け取る。環境2側はあらかじめ環境2側で処理が許された命令または情報のリストを持ち、そのリストを参照して許された命令または情報に対する処理を行う。環境2から環境1への通信は環境2側の視聴用ソフトウェアが特定領域に命令または情報を書き込むことにより行う。環境1側ではこの特定領域を参照することにより命令または情報を受け取り処理する。以上のように環境2側が主導権を持つことにより、悪意を持ったユーザが環境1から不正操作を試みても排除することができる。

【0011】さらに具体的には、環境1と2をそれぞれ独立したOSが管理することにより各環境の独立性を確保する。一台の装置で二つのOSを動作させるための管理とOS間通信の管理とを行う複数OS制御プログラムを設ける。複数OS制御プログラムはOS毎に独立したメモリ領域を割り当て、一方のOSから他方のOSのメモリ領域へのアクセスを防止する。本発明におけるOSとは、プロセス制御機能、プロセススケジューリング機能、割込み制御機能、メモリ管理機能を持つ。したがって、一般的にOSと呼ばれるものに限らず上記特徴を持つものであれば、本発明を適用することは可能である。

【0012】視聴用ソフトウェアなどのアプリケーションソフトウェアについては、ユーザからの操作指示等の入力を受け取り、または、ユーザへのメッセージ出力を行う部分（ユーザインタフェース部）を環境1上に、実際にユーザからの操作指示を実行する部分（コマンド処理部、例えば視聴制御部）を環境2上にそれぞれ構成する。ユーザインタフェース部は環境1側でユーザからの操作を受け取り、上述した環境1と環境2間の通信機能に基づき、環境2側の視聴制御部にユーザからの操作を伝達し、コマンド処理部がユーザの操作に基づく処理を実行する。

【0013】アプリケーションソフトウェアはCD-ROMなどの可搬型記憶媒体を用いて、または他のサーバから通信媒体を用いてネットワーク経由で入手する。導入前のアプリケーションソフトウェアは、環境1上で動作する部分と環境2上で動作する部分と、デジタル署名を持ち、環境1上で動作する部分のプログラムが、上述の環境1と環境2間の通信方法により、環境2側へインストール命令を送信する。環境2側では、デジタル署名を用いて正規のアプリケーションソフトウェアであることを確認したら、インストールを行う。インストールとは、ソフトウェアをコンピュータ上で使用できるように組み込む作業を指す。

【0014】システム起動、システムインストール、アプリケーションソフトウェアの使用許可、コンテンツの使用許可などのために、PCと連携して動作する、物理的及び論理的に内部解析や改ざんを防ぐ耐タンパ性を備えた、ハードウェアモジュールを用いる。ハードウェアモジュールとは、たとえば、PCの拡張ボードや、IC

カード（スマートカード）が該当する。

【0015】視聴用ソフトウェアは一部または全部が暗号化されていてもよい。その場合は、視聴用ソフトウェアの入手とは別の機会に復号鍵を入手すればよい。たとえばPCと、復号鍵を供給するサーバとを通信路で接続し、認証後に、暗号化された通信路を用いてハードウェアモジュールがPC経由で受け取ればよい。ハードウェアモジュールは視聴用ソフトウェアの暗号化された部分を復号する命令を受け取ることにより、環境2上で復号を行う。

【0016】視聴用ソフトウェアは通常、ハードディスクなどの記憶装置上に保存するので、静的な解析を防止するために、一部を暗号化しておいてもよい。さらにデジタル署名を付加することにより、改ざんも防止可能である。視聴用ソフトウェアを暗号化した場合の復号鍵はハードウェアモジュール内に保存しておけばよい。

【0017】視聴用ソフトウェアで処理するコンテンツは、必要に応じて暗号化して配布する。暗号化されたコンテンツの復号鍵は暗号化された視聴用ソフトウェアの復号鍵の入手方法と同様の方法により入手し、ハードウェアモジュール内に保存する。コンテンツを保存する場所は、環境1または環境2のどちらの領域であっても良いし、ハードウェアモジュール内に保存しても良い。

【0018】ハードウェアモジュール内に保存する視聴用ソフトウェアまたはコンテンツの暗号化、復号化に用いる鍵にアクセスする際には、ハードウェアモジュールと環境2上で動作する視聴用ソフトウェアとが、デジタル署名を用いた認証を行い、ハードウェアモジュールが正当であると認めた視聴用ソフトウェアがハードウェアモジュールへのアクセスを行う。これにより、ハードウェアモジュール内の情報を不正に取り出すことを防止可能である。

【0019】システムを正常に起動させるために、起動プログラム（ブートプログラム）も上述の耐タンパ性を備えたハードウェアモジュール内にあらかじめ保存しておく。

【0020】システム起動時には、まず、認証プログラムをPCのメモリ上にロードし、認証プログラムがメモリ上で他の不要なプロセス（たとえば、不正な解析プログラムなど）が動作していないことを確認した上で、ブートプログラムをPCのメモリ上にロードし実行する。ブートプログラムは複数OS制御プログラム、OS1とOS2などのシステムファイルをハードディスクからメモリ上にロードし、必要に応じて、ハードウェアモジュールから暗号化されたシステムファイルの復号鍵を取り出し、PCのメモリ上で復号する。復号後は、各OSは初期設定などを行うことにより、システムの起動が終了する。上述の方法によれば、視聴用ソフトウェアを実行する際のメモリへのアクセスや解析が禁止あるいは制限されるので、視聴用ソフトウェアの改ざん及び解析を防

止することや、コンテンツの著作権保護が可能となる。

【0021】ハードウェアモジュールとしてICカード（スマートカード）などのリムーバブル形式のものを用的場合には、ハードウェアモジュールを持ち運ぶことによって、本発明のシステムが導入されている他の端末であっても視聴権のあるコンテンツを視聴することが可能である。

【0022】上記説明では、コンテンツ視聴用ソフトウェアを例示したが、本発明は、これに限定されることなく、OS上で動作する、不正使用、改ざん、または不正解析の対象となりうる、あらゆるアプリケーションソフトウェアに適用できるものである。

【0023】

【発明の実施形態】（システム概要）図1は本実施例のシステムの構成例である。本実施例のシステムは、1台のPC上で複数OS制御プログラム8がOS1とOS2の2つのOSを制御する。12はPC上のメモリ領域であり、6はOS1が管理するメモリ領域、7はOS2が管理するメモリ領域、複数OS制御プログラム8のメモリ領域を持つ。OS1はハードディスク204a、キーボード205、マウス206を管理し、OS2はハードディスク204b、ハードウェアモジュール3を管理する。ディスプレイ13は複数OS制御プログラム8が表示の排他制御を行うことにより、OS1、OS2の両方から表示可能となっている。さらに、ディスプレイ13と同様の排他制御によりOS1、OS2の両方から出力できるスピーカを備えても良い。10は視聴用ソフトウェアであり、ユーザインタフェース（User Interface、以下UIと称す）部プログラム504と視聴制御プログラム503及び、その他にも設定ファイルなどを持つ。

【0024】複数OS制御プログラム8は、1台のPC上で複数のOSが動作するための各種の制御をする部分で、各ハードウェアの初期化および分割占有処理、OS単位でのCPUのスケジューリング、割り込み処理などを行う。

【0025】各OSはそれぞれ仮想アドレスを実アドレスに変換するためのテーブル（ページテーブルともいう）を持っている。特開平11-149385号公報には、複数OS制御プログラム8がこれらのテーブルの切り替えを行うことにより、特権命令（OS以外では実行できないような保護機能や、メモリ管理機能の設定を行うためのもの）のエミュレーションを行わずに複数のOSを1台のPC上で動作させる方法を開示している。その他、1台のPC上に複数のOSを同時に動作させるための技術としては、PCのハードウェアのエミュレーションを行う仮想計算機と呼ばれる技術がある。これらを本発明の前提条件として、以下説明する。

【0026】本実施例において、2つのOSのうち、一方のOS1はユーザが直接操作する機能を提供するが、

もう一方のOS 2はユーザ11から直接操作する機能を提供しない。さらに、OS間の通信を制御することにより、OS 1からOS 2への直接アクセス機能も提供しない。これらにより、ユーザがOS 2側で動作中のソフトウェアの詳細を知ることができないようにして、OS 2側で動作中のソフトウェアをデバックするなどといった動的解析を防ぐ。

【0027】このようなシステム構成のもと、視聴用ソフトウェア10といった解析されたくないソフトウェアの、実際に視聴の制御を行う視聴制御プログラム503をOS 2上で動作させ、ユーザ11からの操作情報を受け取るUI部プログラム504をOS 1上で動作させる。OS 1はOS 2のメモリ領域を参照できない為、ユーザ11は視聴制御プログラム503がどのように動作しているかを知ることができない。ユーザ11が知ることのできるのは、UI部プログラム504が提供する情報のみである。

【0028】(OS 1とOS 2間の通信) 図4に示すように、それぞれのOSが管理する環境間の通信は、通信制御プログラム501がOS 2参照領域9の内容を参照することにより実現される。システム起動時に複数OS制御プログラム8が、OS 2が使用する上記ページテーブルにOS 1側にあるOS 2参照領域9をマッピングしておくことにより、通信制御プログラム501がOS 2参照領域9を参照することを可能とする。通信制御プログラム501はUI部プログラム504がOS 2参照領域9に書き込んだ内容をコマンドリスト502と比較する。具体的には、UI部プログラム504が情報を受け渡す視聴制御プログラム503に関する情報(プログラム名)、制御情報などをOS 2参照領域9に書き込む。比較した結果、コマンドリスト502にあるコマンドであれば、UI部プログラム504と対となっている視聴制御プログラム503にそのコマンドを受け渡す。なお、UI部プログラム504と視聴制御プログラム503は1対1対応である必要はない。

【0029】コマンドリスト502には、OS 2上で動作中の視聴制御プログラム503が起動時に書き込んだOS 1側からの操作を許可しているコマンドがあり、動作していないソフトウェアのコマンドはない。コマンドリスト502にないコマンドであれば、後述するOS 2からOS 1への通信方法を用いて、エラーメッセージをUI部プログラム504に渡す。UI部プログラム504は、OS 1が提供する機能を用いて表示または音を用いて、ユーザへのエラー通知を行う。

【0030】コマンドリスト502の内容は、OS 2上で動作している視聴制御プログラム503によって変化する。コマンドリスト502の書換えは、新たに視聴制御プログラム503が起動したときに、その起動した視聴制御プログラム503が行う。視聴制御プログラム503は、終了するときに、その視聴制御プログラム50

3に対応したコマンドを、コマンドリスト502から削除する。

【0031】OS 2側からOS 1側への通信は、通信制御プログラム501が視聴制御プログラム503から伝達情報を受け取り、その情報をOS 2参照領域9に書き込むことにより行う。OS 1上のUI部プログラム504は、OS 2参照領域9の内容を参照することによりOS 2側からの情報を受け取る。

【0032】その他の実施例として、視聴制御プログラム503毎にあらかじめコマンドリスト502を設け、通信制御プログラム501は、視聴制御プログラム503毎のコマンドリスト502と比較することにより通信の制御を行うようにしてもよい。コマンドリスト502は、ハードディスクなどの記憶装置に暗号化された状態で保存されていることが望ましい。特開平11-085546号公報に開示されている異種OS上のプロセス間通信を実現する方法を用いても良い。

【0033】(ハードウェアモジュールの機能及び役割) ハードウェアモジュール3は物理的及び論理的に内部解析や改ざんが防衛された鍵管理機能などをもつ耐タンパハードウェアモジュールである。ハードウェアモジュール3の構成を図5に示す。ハードウェアモジュール3は、ハードウェアモジュール3毎に固有の公開鍵暗号方式における秘密鍵301(private key)と、それに対応する公開鍵302と、認定機関の公開鍵310と、複数OS制御プログラム8起動のためのブートプログラム4と、暗号化システムファイル復号鍵303と、認証プログラム5と、鍵管理プログラム19と、コンテンツ鍵17と、ソフトウェア鍵18と、付加情報ファイル305とを耐タンパ性を備えたメモリの不揮発領域309に記憶しておく。

【0034】コンテンツ鍵17は暗号化コンテンツの復号鍵であり、ソフトウェア鍵18は暗号化視聴用ソフトウェアの復号鍵である。付加情報ファイル305とは、コンテンツ鍵17とソフトウェア鍵18とに関連する、有効期限や使用条件などの情報が書き込まれたファイルである。ハードウェアモジュール3はCPU307、メモリ306、外部との通信インタフェース308を持ち、外部からの入力に対する処理を行う。コンテンツそのものを不揮発領域309に記憶しておいても良い。

【0035】ハードウェアモジュール3の外部からハードウェアモジュール3内の情報へのアクセスに際しては、起動時を除き、ハードウェアモジュール3が認証プログラム5をPCのメモリ12上に送信し、アクセスしてきたソフトウェアの認証を行う。認証には公開鍵302または認定機関の公開鍵310を用いる。認証の結果、正しければハードウェアモジュール3は必要な情報をアクセスしてきたソフトウェアに送信し、正しくなければエラーメッセージをアクセスしてきたソフトウェアに送信する。

【0036】PCの起動時におけるハードウェアモジュール3へのアクセスは、ハードウェアモジュール3は認証プログラム5をPCのメモリ12上に送信し、認証プログラム5はPCのメモリ12上に不要なプロセスが動作していないことを確認し、不要なプロセスが動作していなければ、ハードウェアモジュール3からブートプログラム4を取り出し、ブートプログラム4を実行する。不要なプロセスが動作している場合には、起動を停止する。

【0037】また、ハードウェアモジュール3へアクセスするソフトウェアが取り出せる情報を制限する。ハードウェアモジュール3内の情報と、その情報を取り出すことが可能なソフトウェアIDのテーブルをハードウェアモジュール3内に設ける。鍵管理プログラム19は、上記テーブルを利用して、ソフトウェア毎に取り出せる情報を制限する。

【0038】鍵管理プログラム19は、サーバ201からコンテンツ鍵17またはソフトウェア鍵18を取得するときに用いる、ランダムに生成した一時的なセッション鍵の生成、暗号化データの復号の処理や、デジタル署名を用いた認証、後述する鍵の管理を行う。

【0039】ハードウェアモジュール3毎に固有の秘密鍵301は、暗号化ソフトウェアまたは暗号化コンテンツを復号するためコンテンツ鍵17またはソフトウェア鍵18の受け渡しなどに利用する。ハードウェアモジュール3毎の固有の秘密鍵301、公開鍵302を利用することによって、ハードウェアモジュール3毎に異なる暗号をかけてコンテンツ鍵17またはソフトウェア鍵18を配布することが可能であり、また、ソフトウェア、コンテンツの不正使用を防止することが可能であり、また、ユーザ毎に異なるサービスを提供することも可能である。

【0040】ただし、鍵管理プログラム19に、秘密鍵301をハードウェアモジュール3の外部に出力するための命令を用意しないことにより、秘密鍵301がハードウェアモジュール3の外部に出力されることを防ぐ。

【0041】ハードウェアモジュール3は1つのハードウェアモジュール3に上述した全ての機能を含めるのではなく、機能毎に複数のハードウェアモジュール3を用いても良い。例えば、ハードウェアモジュール3を、システムを起動するための情報（ブートプログラム4、認証プログラム5、鍵管理プログラム19、暗号化システムファイル復号鍵303）を持つハードウェアモジュール3Aと暗号化ソフトウェア及び暗号化コンテンツの鍵管理のための情報（認証プログラム5、秘密鍵301、公開鍵302、コンテンツ鍵17、ソフトウェア鍵18、鍵管理プログラム19、付加情報ファイル305）を持つハードウェアモジュール3Bの2つに分けることも可能である。

【0042】コンテンツ鍵17、ソフトウェア鍵18の

管理を行っているハードウェアモジュール3BをICカードのようなリムーバブル形式にすることにより、1台のPCを複数のユーザで共有して、ユーザ毎に異なるコンテンツを視聴することが可能であるし、また、本実施例のシステムが導入されている別のPCにおいてもコンテンツを視聴することが可能である。

【0043】（鍵管理）コンテンツ鍵17とソフトウェア鍵18と暗号化システムファイル復号鍵303の管理は鍵管理プログラム19が行う。鍵管理プログラム19はコンテンツ鍵17またはソフトウェア鍵18を、使用条件などの書かれた付加情報ファイル305に従い管理する。例えば、使用期限のついた鍵の期限が過ぎた場合には、鍵管理プログラム19は鍵管理機能により鍵を削除し、その鍵を利用したコンテンツの視聴やソフトウェアの使用を停止することが可能である。

【0044】この機能を利用することにより、お試し期間を設定し、一定期間だけコンテンツを視聴できるようにしたり、一定期間だけソフトウェアの機能を全て利用できるようにしたりするといったサービスが可能である。コンテンツ鍵17とソフトウェア鍵18及び付加情報ファイル305をハードウェアモジュール3にて管理することにより、ユーザ11が不正に書き換えることを防止可能である。

【0045】（システムのインストール）本実施例のシステムのインストールは、ユーザ11が持つ既存の一般的なPCが備える外部インタフェース（USB、PCカード、拡張ボードなど）にハードウェアモジュール3を接続し、他の媒体（CDROMなど）に格納されているシステムインストールソフトウェア14を用いて行う。

【0046】図2はシステムインストールソフトウェア14の構成例である。システムインストールソフトウェア14は平文システムインストールプログラム221、暗号化システムファイル222、デジタル署名223をもつ。平文システムインストールプログラム221は実行中の不要なプロセスを終了させる機能、ハードディスク204のパーティション分割機能及び本実施例システムをインストールする機能を持つ。暗号化システムファイル222は全体または部分的に暗号化されており、複数OS制御プログラム8、OS2が含まれており、必要であればOS1を含んでいても良い。デジタル署名223は、システムインストールソフトウェア14が改ざんされていないことを確認するために用いるもので、公開鍵302で検証可能に生成されている。したがって、ユーザはインストールに際して、デジタル署名223を検証できる公開鍵302が格納されたハードウェアモジュール3を入手する必要がある。

【0047】図13はシステムインストールの処理の流れである。ステップ1301にて、ユーザ11がPCから平文システムインストールプログラム221を実行することによりインストールが開始される。ステップ13

02にて、平文システムインストールプログラム221は実行中のプロセスの確認を行い、不要なプロセスを終了させ、インストール中に重要な情報が盗まれないようにする。ステップ1303にて、平文システムインストールプログラム221は、暗号化システムファイル復号鍵303を取得するための命令を、ハードウェアモジュール3へ送信する。

【0048】ステップ1304にて、ハードウェアモジュール3は受信した命令を実行する前に、認証プログラム5をPCのメモリに送信する。認証プログラム5は平文システムインストールプログラム221及び暗号化システムファイル222のハッシュ値を計算し、計算結果とデジタル署名223をハードウェアモジュール3に送信する。鍵管理プログラム19は送信された計算結果及びデジタル署名223と公開鍵302を用いて署名検証を行い、正しければ暗号化システムファイル復号鍵303を平文システムインストールプログラム221に渡し、次のステップに進む。正しくなければ、エラーメッセージを平文システムインストールプログラム221に渡し、インストールを中止する。

【0049】ステップ1305にて、平文システムインストールプログラム221は暗号化システムファイル復号鍵303を用いて、暗号化システムファイル222の復号を行う。ステップ1306にて、平文システムインストールプログラム221は復号後の暗号化システムファイル222の中にある設定ファイルを参照しながらシステムのインストールを行う。なお、暗号化システムファイル222の中にシステムインストールプログラムを入れておき、暗号化システムファイル221の復号後は、暗号化システムファイル222の中のシステムインストールプログラムがシステムのインストールを行っても良い。

【0050】平文システムインストールプログラム221はOS1用およびOS2用に領域を確保するためにハードディスク204のパーティション分割を行い、OS1用に確保された領域204aには本実施例のシステム導入前にインストールされていたOS1を含めハードディスク上の情報を全て移し、OS2用に確保された領域204bには新たにOS2のインストールを行う。複数OS制御プログラム8はOS1およびOS2のどちらの領域に書き込んでも良いし、新たに領域を確保して書き込んでも良い。また、ハードディスクドライブを複数台備えたPCの場合は、パーティション分割せずに、領域204a、204bをそれぞれ別ドライブに割り当てても良い。

【0051】ユーザ11による解析および改ざんを防止するために複数OS制御プログラム8、OS2の全体または一部を暗号化してハードディスク上に書き込むことが望ましい。同様にOS1も暗号化してハードディスクに書き込んでも良い。また、システムを正常に起動させ

るために平文システムインストールプログラム221はブートプログラム4をハードウェアモジュール3内に書き込む。ハードディスクのマスターブートレコードに、ハードウェアモジュール3から起動するためのプログラムなど必要な情報を書き込んでおく。

【0052】なお、本実施例のシステムのインストールはPCに予めOS1がインストールされていることを前提としているが、OS1が予めインストールされていなくても、本実施例のシステムを導入することが可能である。さらに、上記システムのインストール方法は本実施例のシステムに限らず、1台のPC上に1つのOSをインストールする方法としても利用可能である。

【0053】(システムの起動) 本実施例のシステムが起動するまでの処理を図3に示す。ステップ231、232にて、ユーザ11がPCの電源を入れることにより、PCのCPUはハードディスクのマスターブートレコードにあるプログラム(初期プログラム)を呼び出す。このプログラムはハードウェアモジュール3内の認証プログラム5をPCのメモリ上にロードする。認証プログラム5は他の不要なプロセスが動作していないことを確認する。他の不要なプロセスが動作している場合には起動を停止し、動作していない場合には認証プログラム5はハードウェアモジュール3からブートプログラム4をPCのメモリ上に読み込み、ブートプログラム4を実行する。

【0054】不要なプロセスが動作していないことを確認することにより、不正なユーザが、例えば起動監視プログラムのようなものを実行させたあとで認証プログラムを呼び出すようにマスターブートレコードを書き直し、重要な情報(暗号化システムファイル復号鍵)を盗むことを防止する。ステップ233、234にて、ブートプログラム4はPCのハードディスクから暗号化システムファイルをPCのメモリ上にロードし、さらにハードウェアモジュール3から暗号化システムファイル復号鍵303を取り出し、暗号化システムファイルの復号を行う。

【0055】ステップ235にて、まず、複数OS制御プログラム8が各OSのメモリ領域を割り当て、それぞれの領域にOS1及びOS2のシステムファイルを配置する。複数OS制御プログラム8はOSの切り替えの制御を行い、各OSは制御が自分に移ったときにそれぞれに必要な初期設定及びプログラム、データなどをメモリにロードすることにより、起動が終了する。起動が終了すると、PCはユーザ11がOS1上で操作できる状態となる。

【0056】(視聴用ソフトウェアのインストール前の構造) 本実施例のシステムで利用する視聴用ソフトウェア10は、予めその一部を、異なる視聴用ソフトウェア個々に固有の鍵を用いて、部分的に暗号化しておく。視聴用ソフトウェア10のインストール前の構成例を図6

に示す。視聴用ソフトウェア10はOS1用インストーラ311、OS2用インストーラ312、暗号化ソフトウェア313、デジタル署名16を持つ。OS1用インストーラ311はOS2へ視聴用ソフトウェア10のインストール要求を出す機能を持ち、OS1上で動作するプログラムである。OS2用インストーラ312はOS2上で動作するプログラムであり、ハードウェアモジュール3からソフトウェア鍵18を取り出す機能を持つ。暗号化ソフトウェア313はOS2上に視聴用ソフトウェア10をインストールするためのソフトウェアである。

【0057】なお、OS1用インストーラ311、OS2用インストーラ312、暗号化ソフトウェア313はそれぞれプログラム、データファイル、設定ファイルなどの複数のファイルを持つ。また、暗号化ソフトウェア313は全てが暗号化されている必要はなく、解析されたくない部分だけを暗号化していても良いし、使用制限、機能制限を行うために部分的に暗号化していても良い。さらに、暗号化は全てに共通の鍵を用いる必要はなく、視聴用ソフトウェア10を構成するファイル毎もしくは機能毎に別々の鍵を用いてもよい。デジタル署名16は、視聴用ソフトウェア10の改ざん検知に利用する。また、視聴用ソフトウェア10の改ざんのみを許さないという場合には、特に視聴用ソフトウェア10を暗号化する必要はなくデジタル署名16を用いて改ざん検知を行う。

【0058】本実施例のシステムに対応した視聴用ソフトウェア10の配布形態は、既存のソフトウェアと同様に、インターネットなどのネットワーク経由での配布、リムーバブルメディアによる配布など、どのような形態であっても良い。また、本実施例では視聴用ソフトウェアを例としているが、それ以外の解析、改ざんを防止したいソフトウェアであっても良い。

【0059】(ソフトウェア鍵の取得) ソフトウェア鍵18の取得方法を図7に示す。ソフトウェア鍵18の取得は、視聴用ソフトウェア10のインストール時もしくは視聴用ソフトウェア10の暗号化されている部分を復号する必要が初めて生じた場合に行う。ステップ321において、視聴用ソフトウェア10はサーバ201にハードウェアモジュール3毎に固有の公開鍵302(KPと記す)及び公開鍵証明書(公開鍵302と併せて保存されていても良い)と、視聴用ソフトウェアが備えているID情報を送る。サーバ201側では公開鍵証明書により、正規のハードウェアモジュールであるかどうかの認証を行う。

【0060】ステップ322において、サーバ201側は一時的なセッション鍵Ks1(共通鍵)を生成し、受信した公開鍵302(KP)を用いて暗号化した結果を、ユーザ11のPCに送信する。ユーザ側のPCでは、視聴用ソフトウェア10が受信データを受け取り、

ハードウェアモジュール3に受信データを送信する。

【0061】ステップ323において、ハードウェアモジュール3内の鍵管理プログラム19は秘密鍵301を用いて、そのデータの復号を行いKs1を得るとともに、一時的なセッション鍵Ks2(共通鍵)を生成し、セッション鍵Ks1を用いて暗号化してサーバ201に送信する。ステップ324において、サーバ201は、受信データをKs1を用いて復号しKs2を得るとともに、ソフトウェア鍵18(Ksoftと記す)とその他の付加情報(使用条件など)を、セッション鍵Ks2を用いて暗号化して、ユーザ11のPC12に送信する。

【0062】ソフトウェア鍵18(Ksoft)のみを送るのであれば、公開鍵302(KP)を用いてソフトウェア鍵18(Ksoft)を暗号化してユーザ11のPCに送信しても良い。ユーザ11のPCでは、視聴用ソフトウェア10は、受信したデータをハードウェアモジュール3内またはPCのハードディスク上に書き込む。ハードウェアモジュール3内に書き込む場合は、特に暗号化する必要はないので、ハードウェアモジュール3内でセッション鍵Ks2を用いて復号して書き込んでよい。一方、PCのハードディスク上に書き込む場合には暗号化した状態で書き込み、ハードウェアモジュール3内にはセッション鍵Ks2を書き込む。このとき一旦、セッション鍵Ks2を用いて暗号化されたソフトウェア鍵18(Ksoft)、付加情報を復号し新たに鍵を生成して暗号化しなおしても良い。

(視聴用ソフトウェアのインストール) 視聴用ソフトウェア10のインストールの処理の流れを図6、図8を用いて説明する。ステップ331にて、ユーザ11がOS1用インストーラ311を起動する。ステップ332にて、OS1用インストーラ311はOS1側にあるOS2参照領域9に視聴用ソフトウェア10のインストールを行う命令を書き込む。この命令にはOS1側にある視聴用ソフトウェア10の全部またはOS2上でインストールに必要なファイルの移動またはコピーの命令およびOS2用インストーラ312を起動する命令を含む。ステップ333にて、通信制御プログラム501がOS2参照領域9を参照して書き込まれている命令を実行する。

【0063】以下の作業はOS2上で行われ、視聴用ソフトウェア10はOS2上にインストールされる。ステップ334にて、OS2用インストーラ312は、まずハードウェアモジュール3に対して、インストールしようとする視聴用ソフトウェアに対応したソフトウェア鍵18を持っているかどうかを問い合わせる。このときハードウェアモジュール3は認証プログラム5をPC12のメモリに送信し、認証プログラム5が、視聴用ソフトウェアのハッシュ値を計算してデジタル署名16と共にハードウェアモジュール3に送る。鍵管理プログラム19は、送られてきたハッシュ値と認定機関の公開鍵3

10とデジタル署名16を用いて視聴用ソフトウェア10の認証を行い、正当な場合にのみ問合せを受け付ける。正しくない場合にはエラーメッセージをOS2用インストーラに送信する。OS2側に認証プログラムを用意しておき、ハードウェアモジュール3へのアクセスが発生したときに、その認証プログラムが視聴用ソフトウェア10の認証を行ってもよい。

【0064】ハードウェアモジュール3がソフトウェア鍵18を持っていない場合には、OS2用インストーラ312がサーバ201からソフトウェア鍵18を取得して、ハードウェアモジュール3に渡す。その後、OS2用インストーラ312は、ハードウェアモジュール3に復号するための命令を送信する。ハードウェアモジュール3がソフトウェア鍵18を持っている場合にはサーバ201への問い合わせをせずに、ハードウェアモジュール3に復号するための命令を送信する。

【0065】ステップ335にて、ハードウェアモジュール3は対応するソフトウェア鍵18をOS2用インストーラ312に送信し、OS2用インストーラ312は復号を行う。本体部は必要な部分だけ復号し、インストール時に復号する必要のない部分は暗号化したままの状態にしておく。また、いったん復号して新たに鍵を生成して再度暗号をかけなおしてもよい。視聴用ソフトウェア10が暗号化されていない場合や、インストール時に復号する必要のない場合には、デジタル署名16を用いた認証を行い、インストールを行う。初めて復号を行う必要が出たときに、ハードウェアモジュール3に対して、ソフトウェア鍵18を持っているかどうかを問い合わせ、持っていない場合にはサーバ201に問い合わせることによって、対応する鍵を取得する。

【0066】インストーラは、図9に示すようにOS1側のハードディスク204aにUI部プログラム504を、OS2側のハードディスク204bに本体起動プログラム342、暗号化ソフトウェア343、デジタル署名344を保存する。本体起動プログラム342は暗号化ソフトウェア343を復号し、実行する機能をもつ。暗号化ソフトウェア343は視聴制御プログラム503を含む、視聴用ソフトウェア10の各種ファイルが暗号化されたものである。暗号化ソフトウェア343とデジタル署名344はOS1側に書き込んでおいても良い。これらのファイルは全て別々のファイルでなければならないということはなく、1つのファイルの中で分割しておいても良い。

【0067】視聴用ソフトウェア10が暗号化されていない場合は、OS1側にUI部プログラム504、OS2側に平文ソフトウェア本体とデジタル署名344を書き込むだけで良い。デジタル署名344は、あらかじめインストールソフトウェアの中に組み込んでおいても良いし、インストール時に新たに作成しても良いし、これらを併用しても良い。インストール時に作成する場

合、インストール後のソフトウェアのハッシュ値を計算し、これをハードウェアモジュール3に送信して、ハードウェアモジュール3内の秘密鍵301によって暗号化し、デジタル署名344を作成する。

【0068】また、OS1側に書き込まれるファイルとOS2側に書き込まれるファイル、すなわちUI部プログラム504と本体起動プログラム342、暗号化ソフトウェア343は、必ずしも1対1に対応している必要はない。UI部プログラム504は、ユーザ11へのインタフェースを提供しているもので変更、交換しても、セキュリティには影響しない。OS2側上で動作するソフトウェアのインタフェースを公開することにより、ユーザ11はUI部プログラム504を自由に作成することが可能である。

【0069】(視聴用ソフトウェアのライセンス契約) 視聴用ソフトウェア10のライセンス契約の方法は、視聴用ソフトウェア10が暗号化されている場合とされていない場合とに分けることができる。視聴用ソフトウェア10が暗号化されている場合、復号鍵を取得するときにライセンス契約を行うことが可能である。視聴用ソフトウェア10が暗号化されていない場合でライセンス契約が必要な場合には、視聴用ソフトウェア10のライセンス契約をしたか、していないかを判断する部分にデジタル署名をつける。

【0070】鍵管理プログラム19は、このデジタル署名を秘密鍵301を用いてハードウェアモジュール3内で作成し、ハードディスク上またはハードウェアモジュール3内に書き込む。ライセンス契約が結ばれた場合には、ライセンス契約をしたか、していないかを判断する部分を書換えるとともに、デジタル署名も付けなおす。デジタル署名を用いることにより、ユーザ11による改ざんを防止でき、ユーザ11が不正に視聴用ソフトウェア10を利用することを防止できる。

【0071】(視聴用ソフトウェアの起動) 視聴用ソフトウェア10の起動の流れを図10に示す。ステップ401にて、ユーザ11がUI部プログラム504を実行することにより、UI部プログラム504はOS2参照領域9に本体起動プログラム342を起動する命令を書き込む。UI部プログラム504の起動は、ファイル管理ソフトウェアを用いたり、画面上のアイコンを操作することなどにより行う。ステップ402にて、通信制御プログラム501がOS2参照領域9を参照し、本体起動プログラム342を実行する。ステップ403にて、本体起動プログラム342は暗号化ソフトウェア343を復号するために、ハードウェアモジュール3からソフトウェア鍵18を取り出し、暗号化ソフトウェア343を復号する。復号された暗号化ソフトウェア343は視聴制御プログラム503及び各種設定ファイルなどに分かれる。

【0072】このとき、ハードウェアモジュール3は、

まず、本体起動プログラム342の認証を、デジタル署名344を用いて、上述のステップ1304と同様に行い、認証できれば命令を受け付けて、ソフトウェア鍵18を本体起動プログラム342に送信する。具体的には、ハードウェアモジュール3は受信した命令を実行する前に、認証プログラム5をPCのメモリに送信する。認証プログラム5は本体起動プログラム342及び暗号化ソフトウェア343のハッシュ値を計算し、計算結果とデジタル署名344をハードウェアモジュール3に送信する。鍵管理プログラム19は送信された計算結果及びデジタル署名344と公開鍵302を用いて署名検証を行い、正しければソフトウェア鍵18を本体起動プログラム342に渡し、次のステップに進む。正しくなければ、エラーメッセージを本体起動プログラム342に渡し、起動を中止する。

【0073】本体起動プログラム342の認証は、OS2側にあるハードウェアモジュール3のデバイスドライバ、もしくは認証プログラムを用いて行ってもよい。また、暗号化ソフトウェア343の一部が暗号化されている場合においても起動時に暗号化部を復号する必要がない場合や使用条件によりある特定の機能を使用できない場合には、暗号化部はそのままにしておき、視聴用ソフトウェア10を起動しても良い。この場合は必要なときに使用条件に反していなければ暗号化部を復号する。

【0074】ステップ404にて、視聴制御プログラム503が設定ファイルを読み込み、視聴用ソフトウェア10の起動が終了したメッセージをUI部プログラム504に送信する。UI部プログラム504がメッセージを受け取った段階で、ユーザ11による視聴のための操作を待つ状態となる。

【0075】(視聴用ソフトウェアの制御) 視聴用ソフトウェア10の起動後は、視聴制御プログラム503が、OS1側から視聴制御プログラム503を制御するためのコマンドを、コマンドリスト502に追加する。ここで追加するコマンドは視聴制御プログラム503が一時的に書き込むものであり、終了時はコマンドリストから削除する。UI部プログラム504は、ユーザ11からの操作(コンテンツの再生、停止、コンテンツタイトルの選択など)を受け取り、OS2参照領域9に視聴制御プログラム503の制御コマンドを書き込む。書き込まれたコマンドを通信制御プログラム501が読み取り、コマンドリスト502に載っているコマンドであれば、視聴制御プログラム503にコマンドを受け渡す。コマンドリスト502に載っていないコマンドであれば、通信制御プログラム501はエラーメッセージをOS2参照領域9に書き込み、UI部プログラム504に受け渡す。UI部プログラム504は、OS1が提供する機能を用いて表示または音を用いて、ユーザへのエラー通知を行う。

【0076】視聴制御プログラム503は受け取ったコ

マンドを処理し、必要であれば結果を画面出力あるいは音出力などを行う。このときのデバイスの制御はOS2が行う。

【0077】画面出力及び音出力に利用するデバイス(サウンドボード、ビデオボードなど)をOS1及びOS2の両方からアクセスを行うために、複数OS制御プログラム8がこれらのデバイスの排他制御を行う。具体的には、複数OS制御プログラム8がデバイスの制御権を管理する。各OSはこれらのデバイスを使用する必要が出た場合に、複数OS制御プログラム8に割込みを発生させ、複数OS制御プログラム8はデバイスの制御権を切替える。

【0078】(コンテンツの配布) コンテンツの配布にはリムーバブルメディアによる配布、通信メディアまたは放送メディアによる配布など様々な形態が考えられる。コンテンツが有料である場合や視聴に制限のある場合など必要に応じてコンテンツを暗号化して配布する。コンテンツを暗号化して配布する場合にはコンテンツ固有の鍵(コンテンツ鍵17)により暗号化する。PC12にコンテンツを保存する場合は、OS1、OS2のどちらが管理する領域に保存しても良いし、ハードウェアモジュール3内に保存しても良い。

【0079】通信メディアまたは放送メディアにより配布されたコンテンツをOS2側またはハードウェアモジュール3内への保存するには、上述の視聴用ソフトウェアと同様の構成を備えたダウンロード用ソフトウェアを設け、ダウンロードと同時にOS2上またはハードウェアモジュール3内に保存することにより可能となる。同様に、OS1上に保存されているコンテンツをOS2上またはハードウェアモジュール3上に保存するには、上述の視聴用ソフトウェアと同様の構成を備えたファイル管理ソフトウェアを設け、OS1上のコンテンツをOS2上またはハードウェアモジュール3上に移動、またはコピーを行うことにより、可能となる。

【0080】さらに、上述のファイル管理ソフトウェアを用いることにより、OS2上またはハードウェアモジュール3上にあるファイルをOS1側から管理することが可能になる。具体的には、ファイルの内容を変更することはできないが、ユーザが再生したいコンテンツを選択して、視聴用ソフトウェア10による再生を行わせたり、ファイル名を変更したりすることが可能になる。

【0081】(コンテンツ鍵の取得) コンテンツ鍵17の取得方法を図11に示す。ステップ411において、暗号化コンテンツを再生する視聴用ソフトウェア10はサーバ201にハードウェアモジュール3毎に固有の公開鍵302(KP)及び公開鍵証明書(公開鍵302と併せて保存されていても良い)と、コンテンツのID情報を送る。サーバ201側では公開鍵証明書により、正規のハードウェアモジュール3であるかどうかの認証を行う。

【0082】ステップ412において、サーバ201側は一時的なセッション鍵Ks1（共通鍵）を生成し、受信した公開鍵302（KP）を用いて暗号化した結果を、ユーザ11のPCに送信する。ユーザ11側のPCでは、視聴用ソフトウェア10が受信データを受け取り、ハードウェアモジュール3内に受信データを送信する。ステップ413において、ハードウェアモジュール3内の鍵管理プログラム19は秘密鍵301を用いて、そのデータの復号を行いKs1を得るとともに、一時的なセッション鍵Ks2（共通鍵）を生成し、セッション鍵Ks1を用いて暗号化してサーバ201に送信する。ステップ414において、サーバ201は、受信データをKs1を用いて復号しKs2を得るとともに、コンテンツ鍵17（Kcと記す）とその他の付加情報（使用条件など）を、セッション鍵Ks2を用いて暗号化して、ユーザ11のPC12に送信する。

【0083】使用条件には鍵の有効期限などの情報が含まれる。また、コンテンツ鍵17（Kc）のみを送るのであれば、公開鍵302（KP）を用いてコンテンツ鍵17（Kc）を暗号化してユーザ11のPCに送信しても良い。ユーザ11のPCでは、視聴用ソフトウェア10は、受信したデータをハードウェアモジュール3内またはPCのハードディスク上に書き込む。ハードウェアモジュール3内に書き込む場合は、特に暗号化する必要はないので、ハードウェアモジュール3内でセッション鍵Ks2を用いて復号して書き込んでもよい。一方、PCのハードディスク上に書き込む場合には暗号化した状態で書き込み、ハードウェアモジュール3内にはセッション鍵Ks2を書き込む。このとき一旦、セッション鍵Ks2を用いて暗号化されたコンテンツ鍵17（Kc）、付加情報を復号し新たに鍵を生成して暗号化しなおしても良い。

【0084】（コンテンツの視聴）コンテンツ視聴までの流れを図12に示す。ステップ421において、ユーザ11の操作によりUI部プログラム504は本体起動プログラム342の起動命令をOS2参照領域9に書き込む。ステップ422において、通信制御プログラム501がこの起動命令をOS2参照領域9から読み込み、本体起動プログラム342を起動する。本体起動プログラム342は暗号化ソフトウェア343を復号して、視聴制御プログラム503を起動させる。ステップ423において、ユーザ11がUI部プログラム504を利用して視聴したいコンテンツタイトルを選択することにより、UI部プログラムがOS2参照領域9にその情報を書き込む。

【0085】ステップ424にて、通信制御プログラム501がその情報を受け取り、視聴制御プログラム503にその情報を渡し、視聴制御プログラム503がコンテンツをハードディスクからPCのメモリ上にロードする。ステップ425において、コンテンツが暗号化され

ている場合、視聴制御プログラム503は、対応したコンテンツ鍵17が存在するかどうかをハードウェアモジュール3に問い合わせ、コンテンツ鍵17が存在しない場合には再生を中止するか、またはコンテンツ鍵17を取得するかどうかをユーザ11に選択させる。

【0086】コンテンツ鍵17を取得する場合には、サーバ201に問い合わせコンテンツ鍵17を取得する。取得後に視聴制御プログラム503はコンテンツ鍵17を取り出すための要求をハードウェアモジュール3に送信する。ハードウェアモジュール3内の鍵管理プログラム19は、付加情報ファイル305に書かれている利用条件のチェックを行い、利用条件を満足する場合に限りコンテンツ鍵17を視聴制御プログラム503に渡す。視聴制御プログラム503は受け取ったコンテンツ鍵17を用いてコンテンツの復号を行う。また、コンテンツが暗号化されていない場合には、ステップ427へ進む。ステップ427にて、視聴制御プログラム503は、コンテンツを再生する。コンテンツが映像の場合であればディスプレイ13に出力する。コンテンツが音を伴う場合であればスピーカにも出力する。

【0087】上述の実施例によれば、改ざんや不正解析を防ぐことが可能になる。加えて、PCのCPUなどの半導体装置や物理デバイスが、耐タンパ性を持つ内部領域に秘密鍵と公開鍵を格納しておき、データの送受信に際して、公開鍵の交換とセッション鍵の受け渡しとセッション鍵によるデータの暗号化を行えば、装置内のバス上を流れるデータを横取りされるという問題を解決することが可能になり、更に高いレベルで改ざんや不正解析を防ぐことが可能になる。更に、CPUや各デバイスは自分の持つ秘密鍵を外部に出力せず、プログラム及びデータをハードディスク上に保存する場合にはCPUの公開鍵を用いて暗号化し、読み込むときはCPUの秘密鍵を用いて復号化することが望ましい。

【0088】本実施例によれば、アプリケーションソフトウェアとその動作環境の改ざん、不正操作、不正解析を困難にすることが可能になる。不正なユーザによるアプリケーションソフトウェアの解析、改ざん行為ができないため、著作権保護を考慮に入れたコンテンツ視聴ソフトウェアの場合であれば、コンテンツの著作権を保護することが可能である。著作者は不正コピーなどによる著作権侵害を心配することなく良質のコンテンツを提供することが可能になる。ユーザにとってはPC上で良質のコンテンツを楽しむことが可能となり、ソフトウェアのバージョンアップも可能であることから常に最新の機能およびサービスを利用することが可能になる。メーカーにとっては専用ハードウェアに比べて経費を削減すると共に、新製品およびサービスをユーザに即提供することが可能になる。ICカードなどのリムーバブルメディアを利用することによって、視聴権のあるコンテンツに対しては、別のPCもしくは携帯端末などでもコンテンツ

を視聴することが可能になる。

【0089】

【発明の効果】耐タンパ性を備えた、ソフトウェアやそれを動作させるシステムを提供できる。

【0090】

【符号の説明】

3・・・ハードウェアモジュール、4・・・ブートプログラム、5・・・認証プログラム、8・・・複数OS制御プログラム、9・・・OS2参照領域、10・・・視聴用ソフトウェア、11・・・ユーザ、13・・・ディスプレイ、14・・・システムインストールソフトウェア、16・・・視聴用ソフトウェアのインストール前のデジタル署名、17・・・コンテンツ鍵、18・・・ソフトウェア鍵、19・・・鍵管理プログラム、201・・・サーバ、223・・・システムインストールソフトウェアのデジタル署名、301・・・秘密鍵、302・・・公開鍵、303・・・暗号化システムファイル復号鍵、311・・・OS1用インストーラ、312・・・OS2用インストーラ、313・・・暗号化ソフトウェア、342・・・本体起動プログラム、344・・・視聴用ソフトウェアのインストール後のデジタル署名、501・・・通信制御プログラム、502・・・コ

マンドリスト、503・・・視聴制御プログラム、504・・・UI部プログラム。

【図面の簡単な説明】

【図1】耐タンパソフトウェアシステムの全体図。

【図2】システムインストールソフトウェアの構造を示す図。

【図3】システム起動までの処理を示す図。

【図4】OS1とOS2間の通信方法を示す図である。

【図5】ハードウェアモジュールの構造を示す図である。

【図6】配布ソフトウェアの構造を示す図である。

【図7】ソフトウェア鍵取得までの処理を示す図である。

【図8】ソフトウェアのインストールの処理を示す図である。

【図9】ハードディスク内でのソフトウェアの状態を示す図である。

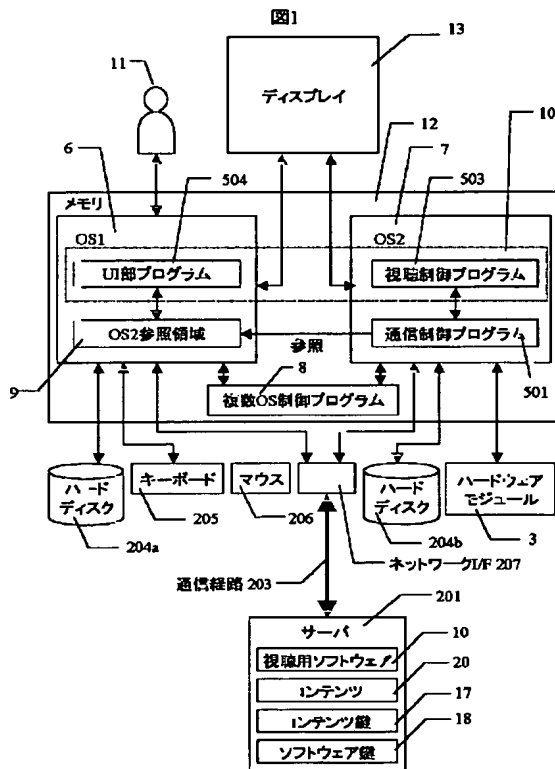
【図10】ソフトウェア起動の処理を示す図である。

【図11】コンテンツ鍵取得の処理を示す図である。

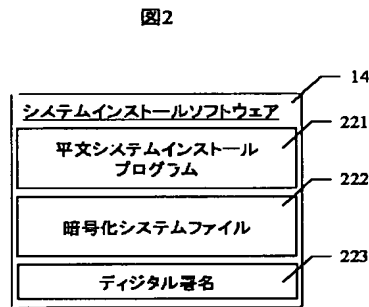
【図12】コンテンツ視聴の処理を示す図である。

【図13】システムのインストールの処理を示す図である。

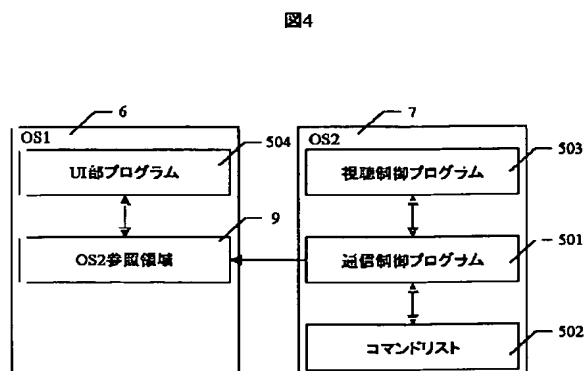
【図1】



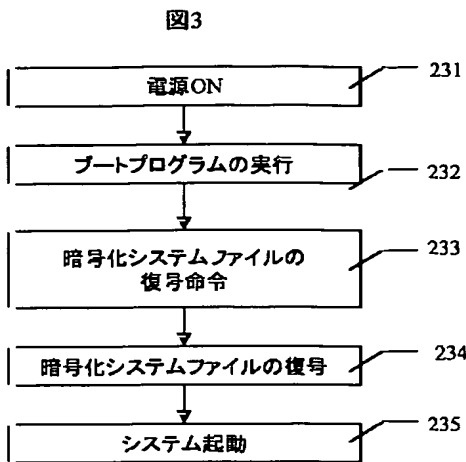
【図2】



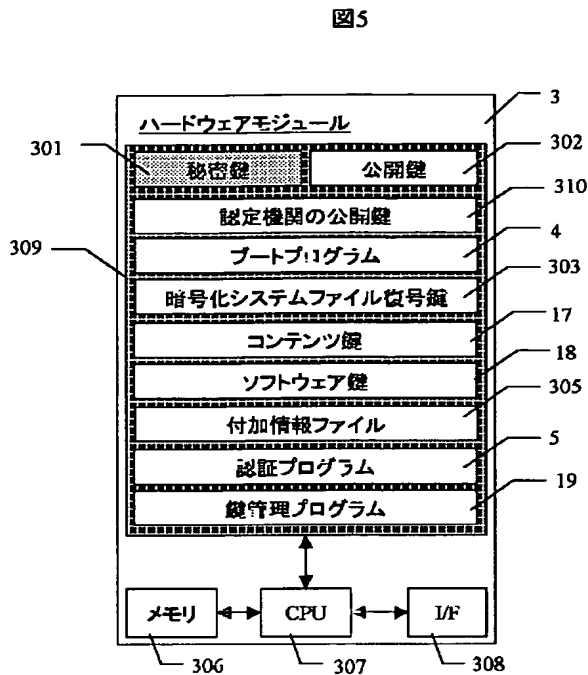
【図4】



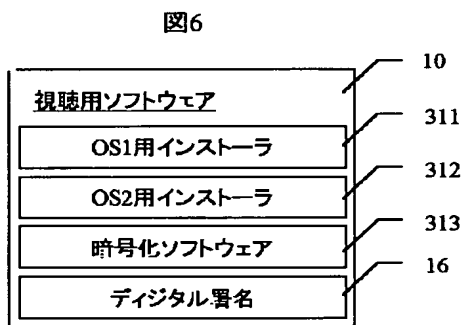
【図3】



【図5】



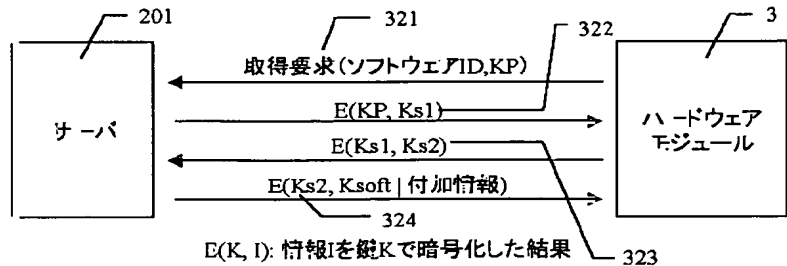
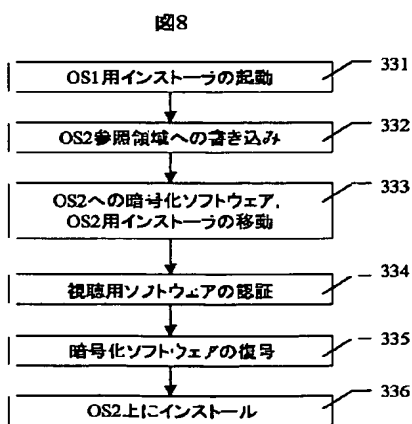
【図6】



【図7】

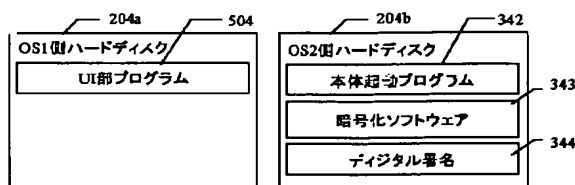
図7

【図8】



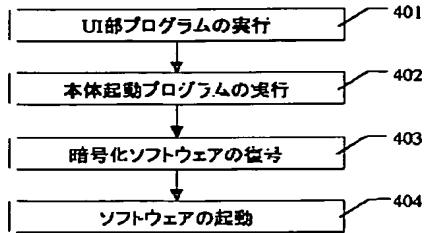
【図9】

図9



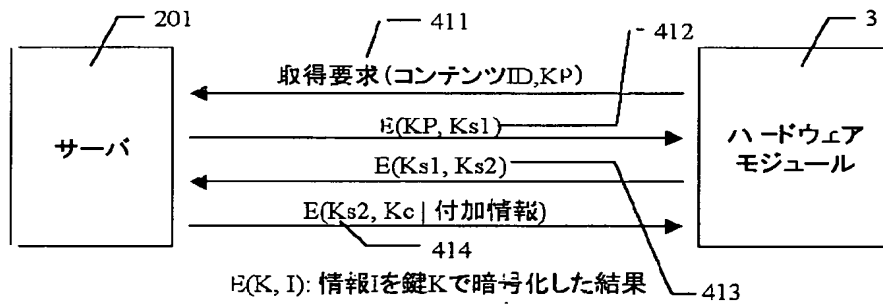
【図10】

図10

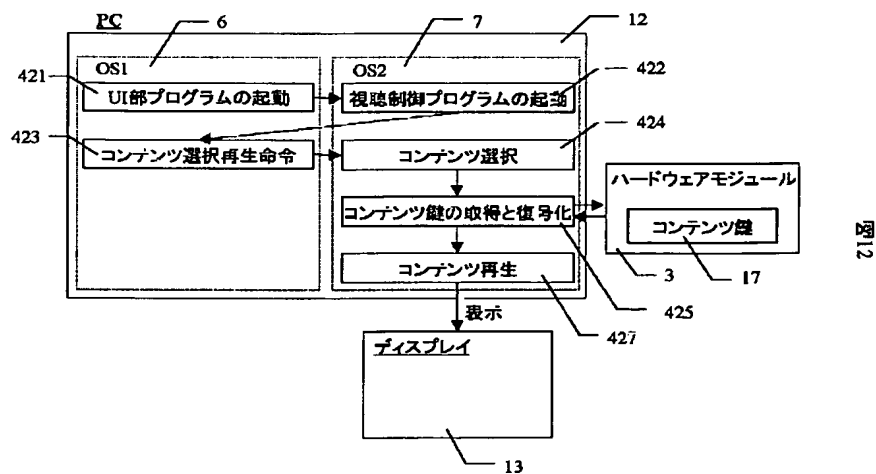


【図11】

図11

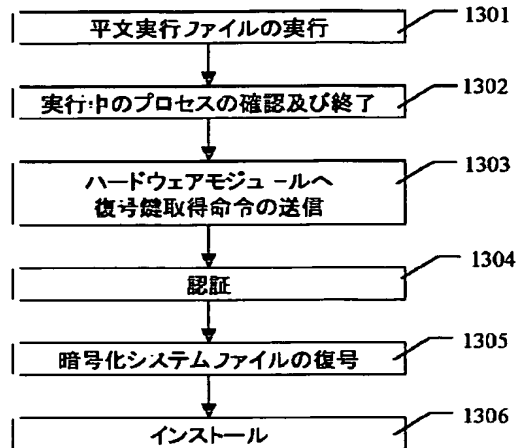


【図12】



【図13】

図13



フロントページの続き

(72)発明者 岡本 宏夫
神奈川県横浜市戸塚区吉田町292番地 株
式会社日立製作所デジタルメディア開発本
部内

Fターム(参考) 5B017 AA03 AA06 BA07 BA09 CA09
CA15
5B035 AA13 BB09 BC00 CA11
5B076 AA13 BA10 FA20 FB02